最大公約数の線形表現 algorithm ALEG
Algorithm for Linear Expression of GCD.

YAMASHITA, Koichiro (kymst)
FMFk(Free Math Forum by kymst)
url: http://kymst.net
GPε (Group Epsilon)

Thu Jul 10 11:48:12 2014 JST

1 ALEG

既に，$a, b \in \mathbb{Z}^+$ について，その最大公約数 $\gcd(a,b)$ が a と b の**整数係数線形結合**として表わされることを我々は知っている：

linear combination on $\mathbb{Z}$

$$\exists \alpha, \beta \in \mathbb{Z} : \gcd(a, b) = \alpha a + \beta b. \tag{1}$$

しかしながら，実際にこの係数 α と β を求めるための計算 (いわゆる Euclidean Algorithm が終了した後の**巻き戻し (Roll Back)**) は，あまり気が進む作業ではない．

話はちがうが，Robert B. Ash という独学で数学を学んだ数学者がいる．現在は America の University of Illinois の名誉教授である (彼の web page が

http://www.math.uiuc.edu/~r-ash/

にある)．その著書に

> *A Primer of Abstract Mathematics.*
> The Mathematical Association of America, 1998. ISBN: 9780883857083

がある．対象とする読者は，抽象的な数学に入っていくための準備をしよう，という，恐らくはこの document を目にする多くの諸君である．

その Chapter 3. Elementary Number Theory の §3.1 The Euclidean Algorithm (pp.45-48) に，以下で説明される algorithm ALEG が記述されている (ただし，ALEG という命名は kymst のデッチアゲである)．最初に読んだときは，余計に煩雑になるのでは? という気がしたが，そうではなかった．Roll Back をより一貫した形で体系的 (systematic) に行なう algorithm である．Ash の言う通り，

> The algorithm to be presented is quite efficient for both hand and machine computation (p.47)

だと思う[*1]．

[*1] やはり Ash の著書 *Basic Abstract Algebra — The Basic Graduate Year —* が，pdf file として公開されている (上記の address から access できる)．その Chapter 2 の §2.5 Polynomial Rings Problems 1-4 (pp. 18f) に再録されている．Solution もあるので心配ない (Solutions Chapter 1-5, p. 9)．今日の document というのはこうでなければいけないと思う．

以下で，**GCD の線形表現 algorithm** (Algorithm for Linear Expression of GCD, ALEG) と名付けてまとめようと思う．

早速，Ash の挙げている例で実行してみよう．

Example 1.1

$a = 123$, $b = 54$ とする．4 個の列 $(q_i)_{i\geq 1}$, $(r_i)_{i\geq -1}$, $(s_i)_{i\geq -1}$, $(t_i)_{i\geq -1}$ を考える：

$$s_{-1} = 1,\ t_{-1} = 0,\ r_{-1} = s_{-1}a + t_{-1}b = 1 \cdot 123 + 0 \cdot 54 = 123$$

とする．これが Table 1 の $i = -1$ の行である：

Table1　Example 1. $a = 123$, $b = 54$.

i	q_i	s_i	t_i	r_i
-1		1	0	123
0		0	1	54
1	2	1	-2	15
2	3	-3	7	9
3	1	4	-9	6
4	1	-7	16	3

次に $i = 0$ の行を作る：

$$s_0 = 0,\ t_0 = 1,\ r_0 = s_0a + t_0b = 0 \cdot 123 + 1 \cdot 54.$$

これで $i = 0$ の行ができた．$r_{-1} = a$, $r_0 = b$ であることに注意せよ．

$i \geq 1$ について，q_i を r_{i-2} を r_{i-1} で割った商と定め，次の漸化式により s_i, t_i, r_i を計算する：

$$s_i = s_{i-2} - q_is_{i-1},\ t_i = t_{i-2} - q_it_{i-1},\ r_i = r_{i-2} - q_ir_{i-1}.$$

各 step を順に説明しよう．

- $i = 1 : r_{-1} = 123$ を $r_0 = 54$ で割れば，商 $q_1 = 2$ を得る．そこで

  $s_1 = s_{-1} - q_1s_0 = 1 - 2\cdot 0 = 1$,　$t_1 = t_{-1} - q_1t_0 = 0 - 2\cdot 1 = -2$,　$r_1 = r_{-1} - q_1r_0 = 123 - 2\cdot 54 = 15$

  となる．
- $i = 2 : r_0 = 54$ を $r_1 = 15$ で割れば，商 $q_2 = 3$ を得るから

  $s_2 = s_0 - q_2s_1 = 0 - 3\cdot 1 = -3$,　$t_2 = t_0 - q_2t_1 = 1 - 3\cdot(-2) = 7$,　$r_2 = r_0 - q_2r_1 = 54 - 3\cdot 15 = 9$.
- $i = 3 : r_1 = 15$ を $r_2 = 9$ で割れば，商は $q_3 = 1$ だから，

  $s_3 = s_1 - q_3s_2 = 1 - 1\cdot(-3) = 4$,　$t_3 = t_1 - q_3t_2 = -2 - 1\cdot 7 = -9$,　$r_3 = r_1 - q_3r_2 = 15 - 1\cdot 9 = 6$.
- $i = 4 : r_2 = 9$ を $r_3 = 6$ で割れば，商は $q_4 = 1$ だから，

  $s_4 = s_2 - q_4s_3 = -3 - 1\cdot 4 = -7$,　$t_4 = t_2 - q_4t_3 = 7 - 1\cdot(-9) = 16$,　$r_4 = r_2 - q_4r_3 = 9 - 1\cdot 6 = 3$.

$r_3 = 6$ は $r_4 = 3$ で割り切られるから，これで Euclidean Algorithm は完了し，$\gcd(a, b) = \gcd(123, 54) = 3$ である．このとき，この最大公約数 $r_4 = 3$ は

$$r_4 = s_4 a + t_4 b = -7 \cdot 123 + 16 \cdot 54 = 3$$

という，元の 2 数 a, b による線形表現として表わされる．■

これまで我々は，Euclidean algorithm によってまず最大公約数を求め，その計算が終了してから，別の作業として線形表現を作ってきた．しかし，この algorithm, ALEG によれば，最大公約数を求める algorithm が，同時に線形表現を作る algorithm にもなっているのである．

2 Proof of Validity

この algorithm, ALEG が妥当であることは，数学的帰納法により容易に証明される．まず，もう 1 度 ALEG を提示し，その後に証明する．

2.1 ALEG

ALEG とは次の計算手順である (以下で colon equal，つまり “`variable` := `value`” は変数 `variable` に値 `value` を代入すること，あるいは左辺を右辺で定義すること，を意味する)：

ALEG

$a, b \in \mathbb{Z}^+$, $a > b$ が与えられたとき，a と b の最大公約数 $\gcd(a, b)$ を求め，更に $\gcd(a, b)$ を a と b の線形結合 $\alpha a + \beta b$ で表わすために，4 個の数列 $(q_i)_{i\geq 1}$, $(r_i)_{i\geq -1}$, $(s_i)_{i\geq -1}$, $(t_i)_{i\geq -1}$ を作る：

Step 1. $s_{-1} := 1$, $t_{-1} := 0$, $r_{-1} := s_{-1}a + t_{-1}b$ とせよ．

Step 2. $s_0 := 0$, $t_0 := 1$, $r_0 := s_0 a + t_0 b$ とせよ．

Step 3. $i \geq 1$ なる i について，r_{i-2} を r_{i-1} で割った商を q_i とし，次の 3 項間漸化式により s_i, t_i, r_i を定めよ：

$$s_i := s_{i-2} - q_i s_{i-1},\ t_i := t_{i-2} - q_i t_{i-1},\ r_i := r_{i-2} - q_i r_{i-1}. \tag{2}$$

Step 3 を r_j が r_{j+1} で割り切られるまで繰り返せ．

Step 4. r_j が r_{j+1} で割り切られたならば，$\alpha := s_{j+1}$, $\beta := t_{j+1}$, $g := r_{j+1}$ として，停止せよ．

このとき，次が成り立つ：

$$\text{Result}: \quad g = \gcd(a, b) = \alpha a + \beta b.$$

Proof.

$i \in \mathbb{Z}^+$ について，$r_i = s_i a + t_i b$ が言えれば十分である．i についての帰納法による．

まず $i = -1, 0$ のときは，定義から明らかである．

$i, i+1$ で成立を仮定する：

$$\text{IH. } s_i a + t_i b = r_i \ \wedge\ s_{i+1} a + t_{i+1} b = r_{i+1}.$$

この第 2 式に q_{i+2} を乗じて第 1 式から引けば次を得る：

$$(s_i - q_{i+2}s_{i+1})a + (t_i - q_{i+2}t_{i+1})b = r_i - q_{i+2}r_{i+1}.$$

(s_i), (t_i), (r_i) の定義から，この式は $s_{i+2}a + t_{i+2}b = r_{i+2}$ に一致する． ■

2.2 One More Example

$a = 221$, $b = 101$ として，gcd を求め，かつそれを $\mathbb{Z}$ 上の a, b の線形結合で表わしてみよう．次の表を得る：

i	q_i	s_i	t_i	r_i
-1		1	0	221
0		0	1	101
1	2	1	-2	19
2	5	-5	11	6
3	3	16	-35	1

$221 \cdot 16 + 101 \cdot (-35) = 1$ となり，$\gcd(221, 101) = 1$ が 221 と 101 の $\mathbb{Z}$ 上の線形結合で表わされた．これは，1 次の不定方程式 $221x + 101y = 1$ が，1 つの特殊解として $(x, y) = (16, -35)$ をもつことを意味する．

若い世代の友人たちが，チョット得した気分になってくれれば，`kymst` は嬉しい．それから，early draft を読んで typo (誤植) を見つけてくれた高校生 R., M. 君，ありがとう:-)

中途半端な世代の同業者のみなさんへ．

コソドロやってんじゃネーヨ!